United States District Court

EASTERN DISTRICT OF OKLAHOMA

In the matter of the search of: **Kik account with the username "jsmith202386"**	**Case No.** **23-MJ-308-DES**

APPLICATION FOR SEARCH WARRANT

I, Meraf Degaga, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the **CENTRAL** District of **CALIFORNIA** *(identify the person or describe property to be searched and give its location)*:

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 21, United States Code, Section(s) 2251 & 2252, and the application is based on these facts:

☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Meraf Degaga
Special Agent
Federal Bureau of Investigation

Sworn to :

Date: 12/6/2023

Judge's signature

City and state: Muskogee, Oklahoma

D. EDWARD SNOW
UNITED STATES MAGISTRATE JUDGE
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Federal Bureau of Investigation ("FBI") Special Agent ("SA") Meraf Degaga, having been first duly sworn, do hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a warrant to search information associated with the Kik account "jsmith202386" using screen name "Jon Smith" (the "SUBJECT ACCOUNT"), further described in Attachment A, that is stored at premises owned, maintained, controlled, or operated by Kik MediaLab.ai Inc. ("Kik" or "MediaLab"), an electronic communications service and/or a remote computing service provider, which is headquartered at 8023 Beverly Blvd. Ste 1144, Los Angeles, California 90048, for the things described in Attachment B.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the user of the SUBJECT ACCOUNT has violated 18 U.S.C. § 2252, which prohibits knowingly possessing, and/or accessing with the intent to view, child pornography (the "TARGET OFFENSES"). There is also probable cause to believe that contraband, evidence, fruits, and instrumentalities of the TARGET OFFENSES, as described in Attachment B, will be found within the SUBJECT ACCOUNT.

3. The facts in this affidavit come from my personal observations, my training, and experience, information from records and databases, and information from other agents and witnesses. This affidavit does not set forth all my knowledge about this matter; it is intended to only show that there is sufficient probable cause for the requested warrant. Unless specifically indicated otherwise, all conversations and statement described in this affidavit are related in

substance and in part only. All dates, times, and ages are approximate. Furthermore, my understating of the facts and circumstances may evolve as the investigation progresses.

AFFIANT'S EXPERIENCE

4. I have been employed as a SA of the U.S. Department of Justice, FBI, since September of 2022, and am currently assigned to investigate crimes occurring in Indian Country, and other federal crimes, at the Muskogee Resident Agency of the Oklahoma City Field Office. While employed by the FBI, I have investigated federal criminal violations related to child exploitation, child pornography, violent crime, and Indian Country matters. I have gained experience through training at the FBI Academy in Quantico, Virginia and experience in conducting these types of investigations. I have received experience in investigating child pornography and child exploitation offenses and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in investigating and enforcing criminal laws, including 18 U.S.C. §§ 1151, 1152, 1153, 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

5. Through my training and experience, I have become familiar with the methods used by people who commit offenses involving the sexual exploitation of children. Through my training and experience, I have gained an understanding of how people who commit offenses relating to the sexual exploitation of minors—including the receipt, distribution, and production of child pornography—use the Internet, computers, and cellular devices to facilitate and commit those offenses.

6. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being

submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

STATUTORY AUTHORITY

7. As noted above, this investigation concerns alleged violations of the following:

a. Receipt of a visual depiction of a minor engaged in sexually explicit contact, codified at 18 U.S.C. § 2252(a)(2) and (b)(1), which prohibits any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct, codified at 18 U.S.C. § 2252(a)(4)(B) and (b)(2), which prohibits any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more book, magazine, periodical, film, video tape, or other matter which contains any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any

means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

DEFINITIONS

8. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code

may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

i. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

j. A "hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

k. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite-based subscription. ISPs

typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

l. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

m. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

n. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

o. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

p. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

t. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-

up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

BACKGROUND ON KIK

9. Kik is a social networking service owned by MediaLab and headquartered in Los Angeles, CA. Kik allows users to create a profile using an email address. The users can then post and share photographs and videos with other users on the platform. Users can also send private messages, photographs, and/or videos to other users. The Kik application is primarily used on a smart device, such as an Apple iPhone, Android cell phone, Apple iPad, or Android tablet.

10. Based on my training, experience, and research, including the investigation to date, and described further below, I know that individuals who view, download, discuss, and/or create child pornography frequently do so using their cellular phones and social media platforms, including Kik. This allows them to both view and store images and/or videos of child pornography on a device that is easily transportable and accessible. Additionally, the use of a smart phone allows individuals to utilize mobile apps, such as Kik, where they can trade images and/or videos of child pornography with other users, and then save these images and/or videos onto their own devices for future viewing or trading with other users.

PROBABLE CAUSE

11. On or about July 3, 2023, I was notified by the FBI, Atlanta Division, that a Kik user, "jsmith202386", screen name "Jon Smith", hereinafter "JON SMITH", was a member of a group in Kik that distributed media files containing child sexual abuse material ("CSAM").[1] JON SMITH was a member of the Kik group named "#youtween". An FBI employee operated an

[1] Kik is an online messaging application that allows users to chat with one another by sending text messages, pictures, and/or videos. The application allows for users to communicate with other users in group chats or direct messages.

undercover Kik account, identified here as OCE-7749. On or about April 28, 2023, OCE-7749 joined the group "#youtween". OCE-7749 learned that JON SMITH was a member of the group "#youtween" on that date. Between in or about April 2023 to May 22, 2023, the FBI employee observed CSAM being distributed in the group "#youtween".

12. On May 11, 2023, JON SMITH posted a link, "https://cosdesbg.ru/invite/i=85226", in "#youtween". OCE-7749 clicked on the link, which led to a web page that read "Teen leak age 5-17" and included a statement about registering for an account to gain access. OCE-7749 registered and obtained access to the content. OCE-7749 observed the content to include media files of suspected CSAM depicting prepubescent minors. On May 22, 2023, the user JON SMITH was removed from the group "#youtween".

13. On July 5, 2023, I received a link via Teleporter, to download and review the suspected CSAM distributed within the "#youtween" chat while JON SMITH was a member. Of the images received, a multitude of photographs and videos are of apparent CSAM. I reviewed some of the photographs and videos and observed the following:

(i) In a video file labeled **8e2fd9ca-30b5-4108-bb75-7f4e434679a6**, there is a prepubescent minor female child, who is topless and pulling down her underwear while dancing. The female's vagina is visible in the video. There is music being played in the background. Flashes of white light appear throughout the video, as if someone is taking photographs behind the camera that is filming the child. The minor is touching herself throughout the video.

(ii) In a video file labeled **e82d35e1-30fc-4afb-8b53-ff6ed60751a1**, there is a prepubescent minor female, who appears to be between the ages of approximately nine and thirteen, who is nude in a vehicle. The child's vagina is exposed. An adult male appears to be

filming himself, while what appears to be him having intercourse with the child. The adult male makes obscene comments to the minor throughout the video. The adult male slaps the child approximately three times and places his hand on the child's neck.

(iii) In a video file labeled **57e63792-e5b3-4489-a40c-af6d409947cb**, there is a prepubescent minor female child laying on her back, on a bed, while watching a children's show on a handheld device she has in one of her hands. The child's vagina is exposed, as she is not wearing pants or underwear. An adult male penetrates her vagina with his erect penis and there appears to be a white, ejaculate-like substance coming from the male's penis, both into and onto the child.

14. On May 3, 2023, JON SMITH posted four images in the "#youtween" group. I reviewed the images and observed the following:

(i) An image file labeled **25f46400-192d-4025-a094-5ec4d2db9d35**, depicted what appeared to be the erect penis of an adult white male.

(ii) An image file labeled **1843f9c7-0b8c-440f-809f-2f554c7f898e**, which appeared to be a prepubescent minor female, with blonde hair and glasses, sticking her tongue out to the camera. There was no nudity in this image.

(iii) An image file labeled **339793ba-4ba8-4b28-bce6-c1f25db1c7ae**, which appeared to be the same minor female described above, smiling to the camera. There was no nudity in this image.

(iv) An image file labeled **5b9986f0-a82f-49de-a023-b710c0ac2fe7**, which appears to be the same minor female described above, leaning over on a bed, exposing the side of her buttocks to the camera. The minor female was wearing a shirt and shorts and her face was not visible in the image.

15. On May 8 and 10, 2023, JON SMITH posted three images on each day in the "#youtween" group. I reviewed the images and observed the following:

(i) Image files labeled **09e46bd8-cafb-46f2-8d89-ac7fc6a17c82** and **326cdc71-1993-42df-aca9-f5cc29b4f875**, which appeared to be a prepubescent minor female, wearing a swimsuit, standing up holding a pool float.

(ii) Image files labeled **456c0a59-c9b0-45b0-8ed5-381351abb64b** and **1d557c3a-20f3-4cae-a08f-af444a987051**, which appeared to be a prepubescent minor female, wearing a swimsuit while lying on a float in a pool. This minor appeared to be the same minor female described above.

(iii) Image files labeled **331a1b31-7762-4f05-b0bd-f841ce3a90b8** and **ee478969-75d1-4e51-9a91-5e172f72235f**, which appeared to be a prepubescent minor female, wearing a swimsuit while lying on a float in a pool.

16. From April 29, 2023, to May 12, 2023, OCE-7749 communicated with JON SMITH on Kik. On April 29, 2023, JON SMITH sent OCE-7749 a message that read, "45 m Arkansas what are u into". On May 4, 2023, OCE-7749 explained to JON SMITH that they were looking for "someone to teach my daughter. You have experience?" JON SMITH replied to OCE-7749 saying, "Yes started with my daughter at 11", which I know from my training and experience implies that he had sexual contact with his daughter when she was a minor. JON SMITH then explained to OCE-7749 that his daughter is now twenty-one, and that his son is now twenty.

17. Based on my calculations, when JON SMITH identified that his daughter was twenty-one in May of 2023, she would have been eleven in 2013, which coincides with the communication to OCE-7749 about when he began sexually abusing his daughter.

18. On May 4, 2023, JON SMITH sent OCE-7749 a picture of two individuals, a male and female sitting on a couch, that matched the ages of the two children he claimed to have. Based on my observations of this image, the female identified as the subject's daughter in this image appears to be the minor female wearing a bathing suit in images in the "#youtween" group on May 8 and 10, 2023.

19. An administrative subpoena was subsequently served to Kik for subscriber information for JON SMITH and Kik returned the following information:

a. Email: jdoe202386@gmail.com

b. Device type: Android

c. Brand: LGE

d. Model: LM-G900

e. IP address: 167.224.242.248

20. An open-source search for the above IP address returned to OzarksGo. (OzarksGo is a telecommunications subsidiary of Ozarks Electric cooperative, offering all-fiber gigabit internet and telephone services to Northwest Arkansas and Northeast Oklahoma.) An administrative subpoena was subsequently served to OzarksGo and returned the following information:

f. Billing Name: Geoff E Luethje

g. Service Address: 78492 S 4671 Rd, Stilwell, OK 74960

h. Telephone number: 918-797-2016 (home); 918-575-1317 (mobile)

21. The subscriber associated with the IP address described above was Geoff Luethje. The address provided for the subscriber was 78492 S 4671 Rd, Stilwell, OK 74960, hereinafter "PREMISES". Utilizing law enforcement databases for a search of the PREMISES further

identified Geoff Edward Luethje, hereinafter "LUETHJE", XX/XX/1977, Social Security number XXX-XX-3513, along with the telephone number 918-575-1317, is associated to the PREMISES.

22. On August 1, 2023, the Honorable Jason A. Robertson, United States Magistrate Judge for the Eastern District of Oklahoma, issued a search warrant for the PREMISES.

23. On August 3, 2023, the FBI executed a search warrant for the PREMISES. LUETHJE and his vehicle were not initially present at the PREMISES at the time of execution of the search warrant. During the execution of the search warrant, LUETHJE returned to the premises and his vehicle was parked across the entryway to the PREMISES on S 4671 Road.

24. LUETHJE then came onto the PREMISES and voluntarily provided that his phone number is 918-575-1317 in an interview with law enforcement. LUETHJE also provided his phone is an Android device, and the passcode for his phone is "3514".

25. Following the interview with law enforcement, LUETHJE stated he wanted to make a call on his phone. LUETHJE acquired the phone from his vehicle. LUETHJE made a call on the phone at or about 7:57 AM. I observed the phone to match the descriptions mentioned above, including the passcode he used to unlock the phone in front of law enforcement. LUETHJE'S phone was seized from his person, after he acquired the phone from his vehicle because there is reasonable belief, probable cause, that CSAM is on the phone.

26. Fearing the imminent destruction of any evidence of a crime that may be located on the phone, agents seized the device to prevent the destruction of evidence. The phone was secured as an item of evidence.

27. After seizure of the phone, LUETHJE voluntarily provided the following information to law enforcement: LUETHJE disclosed to law enforcement that they would find "bad things" on his phone and knew the "bad things" should not be on his device. LUETHJE

admitted that he has utilized the online alias of JON SMITH. LUETHJE confessed that the first time he accessed child pornography through the internet was approximately a year to a year-and-a-half ago. LUETHJE confirmed the possibility that there is child pornography on the phone, stating "there's probably child porn" and it is "on the SD card". LUETHJE provided that he downloaded child pornography from the online chats in Kik that he was part of.

28. A preservation request was processed by Kik on August 7, 2023, for the account associated with the Kik user "jsmith202386" with the preservation number KIK-15050.

29. In my experience conducting these investigations, it is common for possessors, producers, distributors, and/or manufactures of child pornography to have the contraband on social media accounts belonging to him or her.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE, TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

33. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who produce, transport, distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in

children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their pictures, films, video tapes, photographs, magazines, negatives, correspondence, mailing lists, books, tape recordings and child erotica for many years. The Tenth Circuit recognized that "collectors of child pornography are likely to 'hoard' the materials." *United States v. Potts*, 586 F.3d 823, 828-29 (10th Cir. 2009).

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of

forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[2]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

---

[2] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)); *United States v. Frechette*, 583 F.3d 374, 379 (6th Cir. 2009) ("Unlike cases involving narcotics that are bought, sold, or used, digital images of child pornography can be easily duplicated and kept indefinitely even if they are sold or traded. In short, images of child pornography can have an infinite life span.").

SEARCH PROCEDURE

34. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require MediaLab to disclose to the government copies of the Kik records and other information (including the content of communications) particularly described in Attachment B. Upon receipt of the information described in Attachment B, government authorized persons will review that information to locate the items described in Attachment B.

35. In the review of information provided pursuant to this warrant by MediaLab, the government must make reasonable efforts, to the extent required by the Fourth Amendment, to use methods and procedures that will locate and expose those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant while minimizing exposure or examination of irrelevant or attorney-client privileged files to the extent reasonably practicable.

CONCLUSION

36. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated;" 18 U.S.C. § 2711(3) (A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Kik. Because the warrant will be served on Kik, who will then compile the

requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

38. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located on the SUBJECT ACCOUNT specifically described in Attachment A. I respectfully request that the Court issue the proposed search warrant.

Respectfully submitted,

Meraf Degaga
Special Agent
Federal Bureau of Investigation

Sworn to me on December 6, 2023:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

This warrant applies to information associated with the Kik account with the username "jsmith202386", the SUBJECT ACCOUNT that is stored at a premise owned, maintained, controlled and/or operated by Kik c/o MediaLab.ai Inc, which is located at 8023 Beverly Blvd. Ste 1144, Los Angeles, California 90048.

ATTACHMENT B

Property to be seized

To ensure that agents search only the SUBJECT ACCOUNT described in Attachment A, this search warrant seeks authorization to permit employees of Kik c/o MediaLab.ai Inc. ("PROVIDER") to assist agents in the execution of the warrant. To further ensure that agents executing this warrant search only the SUBJECT ACCOUNT described in Attachment A, the following procedures will be implemented:

I. Accounts and Files to be Copied by Provider's Employees

To the extent that the information described in Attachment A is within the possession, custody, or control of PROVIDER, including any messages, records, files, logs, or information that has been deleted but is still available to PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), PROVIDER is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A for the following:

a. All subscriber, contact, and personal identifying information, unrestricted by date, for the SUBJECT ACCOUNT, to include but not limited to full name, user identification numbers, date of birth, gender, contact e-mail addresses, physical addresses (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

b. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account numbers) for the SUBJECT ACCOUNT.

c. All IP logs, including all records of the IP addresses that logged into the SUBJECT ACCOUNT from February 1, 2022, to present.

d. All records or other information regarding the devices and internet browsers associated with, or used in connection with, the SUBJECT ACCOUNT, including the hardware model, operating system version, unique device identifiers, mobile network information, user agent string, and any other Kik accounts not identified as the SUBJECT ACCOUNT but that are linked by common data such as the same device and application ID, IP address, or cookie information from February 1, 2022, to present.

e. All activity logs associated with the SUBJECT ACCOUNT and all other documents showing the posts of the user IDs.

f. All transactional chat logs associated with the SUBJECT ACCOUNT, to include private and group chat messages from February 1, 2022, to present.

g. All images and videos associated (sent or received or otherwise associated) with the SUBJECT ACCOUNT, including the username and IP addresses associated with images and videos sent to or received by the SUBJECT ACCOUNT from February 1, 2022, to present

h. All information generated by or associated with the SUBJECT ACCOUNT, including any postings, status updates, photographs, comments, networks or groups of which the user is a member, and information about the user's access and use of the Kik application.

i. All other records and contents of communications and messages made or received by the SUBJECT ACCOUNT from February 1, 2022, to present, including all public chat messages, private chat messages, chat history (including chat rooms joined or removed from), video and voice calling history, and contact lists.

j. All records of Kik searches performed by the SUBJECT ACCOUNT from February 1, 2022, to present.

k. All records pertaining to communications between the SUBJECT ACCOUNT and any other person regarding the SUBJECT ACCOUNT, including but not limited to any abuse reports associated with the SUBJECT ACCOUNT, contacts with support services, and records of actions taken from February 1, 2022, to present.

l. A date-stamped log showing the usernames that SUBJECT ACCOUNT added and/or blocked from February 1, 2022, to present.

m. All abuse reports associated to the SUBJECT ACCOUNT including the unknown usernames from February 1, 2022, to present.

n. Registration IP address associated to the SUBJECT ACCOUNT.

II. Information to be seized by the government:

All information described above in Section I that constitutes evidence, instrumentalities, contraband, or fruits of violations of 18 U.S.C. § 2252(a)(4)(B), which prohibits knowingly possessing, and/or accessing with the intent to view, child pornography (the "TARGET OFFENSES") involving the Kik username or ID identified in Attachment A (the SUBJECT ACCOUNT) since February 1, 2022, to present, and pertaining to the following matters:

a. Information, electronic records, or correspondence pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

b. Any and all information, correspondence (including emails), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educing, enticing, coercing, or persuading a minor to engage in sexual acts;

c. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums;

d. Any and all electronic and/or digital records and/or documents including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;

e. Information, images, or communications pertaining to a sexual interest in children or in child pornography, including but not limited to erotic writings involving minors;

f. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime(s) under investigation and to the Kik account owner;

g. Evidence indicating the account owner's state of mind as it relates to the crime(s) under investigation;

h. The identity of the person(s) who created or used the SUBJECT ACCOUNT, including records that help reveal the whereabouts of such person(s); and

i. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.